UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/840,472	04/23/2001	John J. Bowe	Zolera/Patent	5737

21034 7590 02/16/2006

IPSOLON LLP
111 SW COLUMBIA
SUITE 710
PORTLAND, OR 97201

EXAMINER	
LANIER, BENJAMIN E	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 02/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/840,472	BOWE ET AL.	
	Examiner	Art Unit	
	Benjamin E Lanier	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-33,56-60,62-82 and 91-104* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-33,56-60,62-82 and 91-104* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 April 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. Applicant's amendment filed 21 December 2005 amends claims 17, 18, 56, 58, 59, 61, 62, 65, 67, 91, 104. Applicant's amendment has been fully considered and is entered.

2. Applicant has stated that claims 1-33, 56-82, and 91-104 are currently pending, but the claim sheet identifies claim 61 as having been cancelled. Therefore, claims 1-33, 56-60, 62-82, and 91-104 are pending.

Response to Arguments

3. Applicant's arguments filed 21 December 2005 have been fully considered but they are not persuasive. It appears that Applicant misunderstood the Examiner's identification of the new matter added to the claims in the amendment filed 16 May 2005. Prior to the amendment file 16 May 2005 the claims were directed to a signature authentication scheme between a server and a single client. The client transmits data to the server, which digitally signs the data and returns the digitally signed data back to the client that originally transmitted the data. At some point thereafter, the client can have the digital signature authenticated by transmitting the digitally signed data back to the server. The amendment filed 16 May 2005 amended the claims to so that two different clients are required in the signature authentication scheme. Now as claimed, after the server digitally signs the data, the server transmits the digitally signed data to a different client that the one that originally transmitted the data. It is this different client that is requesting authentication of the digital signature. As stated in the Office Action mailed 21 June 2005, there is no support in the specification for this amendment to the claims as mentioned above.

4. Applicant states that the specification clearly describes the invention as it relates to a first client signing an electronic document, and a second client later authenticating the signature of the first client. This scheme is not what is claimed. Looking at claim 1 specifically, the claims require a server digitally signing an electronic document. That same server is used to authenticate the signature of the digitally signed electronic document. From claim 1:

> "...generating at the server a signature corresponding to the second client by processing the data object"
>
> "...returning the signed object from the first client to the server to authenticate that the signature of the signed object corresponds to the second client"

Figure 4 of the specification is the only embodiment that appears to use multiple clients, and the detailed description of Figure 4 (pages 14-15) do not support the claims as discussed above.

Claim Objections

5. Claims 92-103 are objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. The above-identified claims are dependent on claim 104, which is improper because claim 104 does not precede the identified claims.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 4, 58, 61, 97-99, 102, 103 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

8. Claims 4, 61, 97-99, 102, 103 recite, "the client", which renders the claim vague and indefinite because it is unclear to which client the claim is referring.

9. Claim 58 recites the limitation "the signing client" in line 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 1-5, 8-33, 56-59, 61, 62-80, 91-104 are rejected under 35 U.S.C. 102(e) as being anticipated by Zabetian, U.S. Patent No. 6,327,626. Referring to claims 1, 2, 11-13, 16-19, 22-24, 56, 57, 59, 64-68, 71-73, 91, 93, 94, 102-104, Zabetian discloses an electronic document verification system wherein a certification provider is provided to verify signed electronic documents (Col. 4, lines 5-6, 11-12), which meets the limitation of the server. The certification provider receives requests from clients to certify an electronic document (Col. 4, lines 52-55), which meets the limitation of receiving the data object transmitted from the second client/signature-requesting client to the server via the computer network. Part of the certification process involves generating the digital signature of the document by the signature generation

means within the certification provider (Co. 4, lines 56-59 & Col. 8, lines 43-47), which meets the limitation of generating at the server a signature corresponding to the second client/signature-requesting client by processing the data object. The user request can be for a certified electronic mail transmission from a sender to a recipient (Col. 11, lines 18-21). The certification provider receives the electronic mail message is received by the certification provider (Col. 11, lines 21-24), and digitally signed (Col. 11, lines 43-51) before being transmitted to the recipient (Col. 11, lines 51-53), which meets the limitation of associating the signature with the data object at the server to create a signed object, delivering the signed object to the first client. The message received by the recipient describes the process by which the message can be verified (Col. 9, line 59 – Col. 10, line 14). After receipt, the message can be verified by transmitting the message to a verification address so that the digital signatures can be compared (Col. 12, line 17 – Col. 13, line 16, 38-49), which meets the limitation of returning the signed object from the first client/signature-verifying client to the server to authenticate that the signature of the signed object corresponds to the second client, obtaining the data object using information contained within the signed object, obtaining the digital signature using informaiton contained within the signed object, means for obtaining the private key stored on the server using information contained within the signed object, the authentication including deriving from the signed object informaiton representative of the data object and the signature, generating a comparison value using the information representative of the data object, and determining whether the comparison value and the at least a portion of the signature meet a pre-determined criteria.

Referring to claims 3, 4, 58, 61, 96, Zabetian discloses that a determination is made before processing the electronic mail document to see if the sender of the electronic mail

document is registered with the system (Col. 6, lines 38-53), which meets the limitation of authenticating the second client/signature-requesting client at the server in connection with the second client/ signature-requesting client transmitting the data object being to the server, wherein the second client/ signature-requesting client is authenticated by the server using information representative of the client.

Referring to claims 5, 97-99, Zabetian discloses that passwords can be used to verify the user's registration (Col. 6, lines 63-64).

Referring to claim 8, Zabetian discloses that the registration process is performed using public key cryptography (Col. 15, lines 29-31).

Referring to claim 9, Zabetian discloses the use of certificates (Col. 9, lines 32-34).

Referring to claim 10, Zabetian discloses that passwords can be used to verify the user's registration (Col. 6, lines 63-64), which meets the limitation of zero knowledge authentication.

Referring to claims 14, 62, 95, Zabetian discloses that during the registration process a document of the requesting user is hashed and then encrypted (Col. 6, line 54 – Col. 7, line 18), which meets the limitation of wherein the step of generating the signature includes the step of assigning a private key to the second client/ signature-requesting client, performing a predefined hash function on the data object to produce a hash total and enciphering the hash total using the private key.

Referring to claims 15, 63, 92, Zabetian discloses that the document can be an email message that contains a source and destination address (Col. 9, lines 40-45), which meets the limitation of the signed object comprises the signature and an address of the data object.

Referring to claims 20, 25, 26, 29-33, 69, 74, 75, 78-82, Zabetian discloses that the signed document contains a timestamp (Col. 9, lines 61-63), which meets the limitation of additional data signed by the server, the additional data is derived by processing the data object using a pre-determined function, the additional data is obtained from a device.

Referring to claims 21, 70, Zabetian discloses that an identification code is used by the server to identify the document and the registered user in a database (Col. 9, lines 1-2).

Referring to claims 27, 28, 76, 77, Zabetian discloses that during the registration process a document of the requesting user is hashed and then encrypted (Col. 6, line 54 – Col. 7, line 18), which meets the limitation of the pre-determined function is a hash function, the pre-determined function is a transform function.

Referring to claim 100, Zabetian discloses that during the registration process a document of the requesting user is hashed and then encrypted (Col. 6, line 54 – Col. 7, line 18), which meets the limitation of wherein the digital signature further comprises an encrypted field, wherein the server generates the encrypted field by hashing the data object according to a predefined hash function to create a hash, and encrypts the hash using the private key assigned to the user. Zabetian discloses that the signed document contains a timestamp (Col. 9, lines 61-63), which meets the limitation of a timestamp.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

14. Claims 6, 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zabetian, U.S. Patent No. 6,327,626, in view of Pavlik, U.S. Patent No. 6,807,633. Referring to claims 6, 7, Zabetian discloses that a determination is made before processing the electronic mail document to see if the sender of the electronic mail document is registered with the system (Col. 6, lines 38-53). Zabetian does not disclose using a SSL encryption channel for the determination. Pavlik discloses a digital signature system where a client is authenticated over a network by way of a SSL secure channel (Col. 6, lines 37-49). It would have been obvious to one of ordinary skill in the art at the time the invention was made to authenticate the client of Zabetian over an SSL secure channel so as to provide a digital signature system with electronic documentation, such as credit card information and/or bank account information as taught in Pavlik (Col. 6, lines 50-53).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805. The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Benjamin E. Lanier

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100